REMARKS

Claims 1-21 and 31-40 are pending. Claims 1, 20, 21 and 31 are amended to more particularly point out the distinctions over the cited art. Claims 2, 3 are canceled. Claims 32-40 are withdrawn.

Election/Restriction

The Examiner has maintained the restriction requirement of the previous office action. Claims 32-40 have been withdrawn from consideration. To preserve the right of appeal, Applicants maintain traversal of the restriction requirement as stated in the previous office action.

35 U.S.C. § 103 Rejection

Claims 1-21 and 31 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Scheifler et al. (US Patent 6,138,238) in view of Colburn et al. (US Patent 6,173,404). Applicants respectfully traverse this rejection.

The Examiner states reliance on the references as follows:

> Scheifler teaches determining whether access to a particular interface (e.g. write to any specific file in the directory, such as "c:/thisfile") case on a call to the first interface (e.g. write to any file in a directory, such as "c:/") (Fig. 1; Fig. 4-6; col. 4, l. 51 to col. 5, l. 3 and col. 9, l. 11 to col. 14, l. 38)
>
> Colburn [sic] the target object (Fig. 8, ref. 160) determine access authorization by checking its own security policies (Fig. 8, ref. 184, 194) (col. 1, l. 12 to col. 3, l. 45; col. 7, ll. 26-52 and col. 11, ll. 25-51). Office Action, p. 4.

As demonstrated below, these stated teachings do not teach or suggest the elements of the claims.

With regard to the Applicants' argument that both Scheifler and Colburn teach using a centralized authority to determine security access, the Examiner states

> the examiner is not fully clear where in either Scheifler or Colburn [sic] teaches centralized authority, as it seems neither Scheifler nor Colburn [sic] disclosed wording such as "central" or "centralized" authorization. Office Action, p. 3.

The concept of centralized comes from examining the structure of the Scheifler's and Colburn's inventions. As stated in Applicants' previous response, neither reference determines security

measures at a target object. In each case, a security determination is made elsewhere; in other words, the determination is made by consulting a resource (be it another object, file, system, etc.) external to the target object.

Colburn, for example, discloses the concept of incorporating an owner identifier into objects. See e.g., col. 12, line 59 – col. 13, line 15. For example, this scheme requires objects to consult the user of the computer, or in the instance of a client-server relationship, consult a remote server for security information. See e.g., col. 13, line 25 – col. 14, line 24. Moreover, Colburn's security measures are determined by "attributes obtained from the call stack to determine whether particular conditions are met to permit an accessing instance to access a particular target." Col. 8, lines 65-67. In other words, the target objects within Colburn do not make any security determinations and certainly do not make any security determinations based on the target object's own security policies. With regard to this argument, the Examiner states

> the examiner is relying on Colburn [sic], not Scheifler, for the teaching/suggesting of the target object determining access authorization, as in accordance to applicant's own argument, the target object determined access authorization by checking its [sic] own security policy (applicant's argument on page 9, lines 26-27), and Colburn [sic] teaches a target object (Fig. 8, ref. 160) having its own security policy (Fig. 8, ref. 184, 194) for determining access authorization to the target object. Office Action, p. 3.

Applicants submit that making a security determination at a target object as claimed is not the same as simply "having" or possessing access authorizations within an object. Taking Colburn as a whole, it is clear that the security structure and functionality is contained not at the target object but elsewhere within the scheme. When a target object is said to "check" its own security policies, it does automatically mean that that target object has a capability to determine its own security policy.

Scheifler discloses the use of permission objects (which are not target objects) "which determine whether a requested permission is authorized by the particular permission represented by the permission object." Col. 11, lines 56-57. The Examiner states

> the examiner is not fully clear why Scheifler's disclosure of implied permission does not constitute determining access to other interface of a target object, as Scheifler teaches the implied permission still need to be determined, in order to have knowledge of access authorization of what is implied. Office Action, pp. 3-4.

First, examining Scheifler as a whole, Applicants submit Scheifler's security determination does not occur at the target object, as presently claimed. The security determination occurs at a permission object (which is implemented as a centralized authority, see e.g., col. 11, line 60 – col. 12, line 55), which teaches away from the present claims. Second, interface permissions in the present invention as claimed are not implied. Each interface may grant varying degrees of access to the target object. See e.g., Specification para. [0058].

Moreover, Scheifler's disclosure of implied permission does not constitute determining access to other interface of a target object as the Examiner implies. Scheifler explicitly states:

> If a permission is represented by a permission object, the validation method for the permission object contains code for determining whether one permission is implied by another. For example, a permission to write to any file in a directory implies a permission to write to any specific file in that directory, and a permission to read from any file in a directory implies a permission to read from any specific file in that directory. However, a permission to write does not imply a permission to read. Col. 12, lines 46-55.

In the present invention, access to one interface does not "imply" access to another interface. See, e.g., Specification, para. [0050]. Third, as Scheifler explicitly states above, the permission object contains code for determining whether one permission is implied by another. The present invention as claimed does not determine whether a permission is implied based on another permission. Rather the target object determines whether an external object access to a particular interface based on a call to the first interface. See e.g., Specification, para. [0058].

Scheifler and Colburn, individually and in combination, teach away from the present invention as claimed. The Examiner states:

> by combining Colburn with Scheifler's above teaching of implied permission, the resulting combination further teaches the target object implementing access authorization in association with implied permission to other interfaces. Office Action, p. 4.

However, teaching "the target object implementing access authorization in association with implied permission to other interfaces" is not what the claim language states. Scheifler and Colburn, individually and in combination, do not teach or suggest each and every element of the claims. Accordingly, the Applicants respectfully request withdrawal of this rejection.

Conclusion

All of the stated grounds of rejection have been properly addressed. Applicants therefore respectfully request that the Examiner reconsider the outstanding rejections and allow the present claims. The Examiner is invited to telephone the undersigned representative if an interview might expedite allowance of this application.

Respectfully submitted,

BERRY& ASSOCIATES P.C.

Dated: December 21, 2009

By: /Shawn Diedtrich/
Shawn Diedtrich
Registration No. 58,176
Direct: 480.704.4615

9255 Sunset Blvd., Suite 810
Los Angeles, CA 90069
(310) 247-2860